Exploiting root-mean-square time-frequency structure for multiple-image optical compression and encryption

Ayman Alfalou, C. Brosseau

Exploiting root-mean-square time-frequency structure for multiple-image optical compression and encryption

A. Alfalou[1,*] and C. Brosseau[2]

[1]*Département Optoélectronique, Laboratory L@BISEN, ISEN-BREST, 20 rue Cuirassé Bretagne, CS 42807, 29228 Brest Cedex 2, France*

[2]*Université Européenne de Bretagne, Université de Brest, Lab-STICC and Département de Physique, CS 93837, 6 avenue Le Gorgeu, 29238 Brest Cedex 3, France*

**Corresponding author: ayman.al-falou@isen.fr*

Received January 22, 2010; revised April 18, 2010; accepted May 11, 2010; posted May 17, 2010 (Doc. ID 123188); published May 28, 2010

We report on an algorithm to compress and encrypt simultaneously multiple images (target images). This method, which is based upon a specific spectral multiplexing (fusion without overlapping) of the multiple images, aims to achieve a single encrypted image, at the output plane of our system, that contains all information needed to reconstruct the target images. For that purpose, we divide the Fourier plane of the image to transmit into two types of area, i.e., specific and common areas to each target image. A segmentation criterion taking into account the rms duration of each target image spectrum is proposed. This approach, which consists of merging the input target images together (in the Fourier plane) allows us to reduce the information to be stored and/or transmitted (compression) and induce noise on the output image (encryption). To achieve a good encryption level, a first key image (containing biometric information and providing the intellectual property of the target images) is used. A second encryption key is inserted in the Fourier plane to ensure a relevant phase distribution of the different merged spectra. We also discuss how the encoding information can be optimized by minimizing the number of bits required to encode each pixel.

OCIS codes: 100.5010, 100.2000, 100.3008.

The increased use of multimedia applications, e.g., the exchange of images or video clips, requires that the amount of data be reduced in order to be easily transmitted and/or stored (data compression). Another important aspect of this issue is that, often, the transmitted data should be secured (data encryption). Specifically, we are interested in Internet Protocol (IP)-based video surveillance, which has been a popular security tool for years. One possible application of this study is to use a video system of network cameras to detect various posture-based events in a typical elderly monitoring application in a home surveillance scenario. These events include normal daily life activities and unusual events, e.g., fall detection. When a fall happens, the alert goes out and a video sequence showing the scene is sent to a medical response team. Image compression of the video sequence is mandatory to reduce its size. To preserve privacy, encryption can be also realized so that only authorized persons can view the scene. Achieving compression and encryption operations can be implemented using optical techniques (see [1], for a review), taking advantage of the parallelism achievable with optical processing, the natural two-dimensional (2D) imaging capabilities of optics, and the potential of the algorithms and optoelectronic interfaces suitable for optical information processing. However, the data compression and encryption operations are often performed independently of each other. These two operations, if realized independently, may yield a serious incompatibility issue.

In their pioneering work on double random phase (DRP) encoding, Réfrégier and Javidi [2] proposed an encryption method based on the $4f$ setup and on multiplication of the target image and its spectrum by two random phase keys [2]. However, this Fourier plane encoding algorithm affects the size of the file to be transmitted and/or stored. Thus, applying a compression method to the data may result in poor quality of the reconstructed image [1]. By way of consequence, using this algorithm for the above-mentioned video surveillance leads to degraded performance for fall detection, because the images have poor quality. Furthermore, the DRP encryption scheme can be considered potentially insecure against several possible attacks [3]. The authors of [3] proposed some possible improvements to this approach, i.e., large keys, of at least 1000×1000 pixels, should be used and encryption keys should be changed regularly. This leads to an increase in the algorithm's complexity and in the amount of data required to reconstruct the target image. Furthermore, the encryption keys should be changed periodically. Hence, the recipient should have a large number of decryption keys and be able to know what encryption key was used by the sender. To overcome this problem, an improved encoding algorithm adapted to the multiple-image problem was proposed by Yong-Liang and co-workers [4]. In an earlier work [5], we also proposed adding an encryption step to the classical DRP scheme. This encryption, based on the iterative Fourier transform (FT) renders the DRP more resistant to attacks, permits reducing the information to transmit, and is adapted to the multiple-image issue. However, it may be hard to put this technique into practice due to the increase in the algorithm's complexity, especially for secure real-time applications.

In this Letter, we propose, analyze, and demonstrate a simple algorithm to simultaneously compress and encrypt multiple images. This study focuses on a specific algorithm that is based upon a spectral multiplexing operation, i.e., fusion without overlapping of multiple images aimed to achieve a single encrypted image at the output plane of our system, and that contains all the information needed

to reconstruct the target images. As will be shown below, the Fourier plane of the resulting image is partitioned into several areas according to a segmentation criterion that takes into account the respective weight of each area for the target image reconstruction. In the next step, this area is applied to the most important target image. In this Letter, the strength of the algorithm is tested and we present clear evidence that this algorithm is well suited to the context of multiple-view video sequences for which the images are very similar. To do this, we adapt the $4f$ setup to multiplex spectra of different target images. This multiplexing is based on the use of an adapted version of the segmentation criterion used to fabricate multicorrelation composite filters [6]. This criterion consists of dividing the Fourier plane into different kinds of areas: a first area common to the different spectra, i.e., for which the different images have similar spectra (these areas being more or less important depending on the degree of resemblance between the target images), and other areas specific to the target image spectra (for each area, information specific to the target image spectrum is introduced). Two important points are considered to elaborate this criterion. (i) For a given pixel of an image A, the energy criterion compares its frequency energy normalized by the total energy of its spectral plane with the frequency energy normalized of the same pixel for an image B [6]. (ii) The correlation filter is multiplied by a bandpass function P [7,8].

The synoptic diagram of our algorithm is shown in Fig. 1. For illustrative purpose, we choose to consider an example that consists of simultaneously encrypting and compressing two target images I_1 and I_2 (Fig. 1). Our algorithm involves the following steps. We first perform the FT of each image separately. Then, each spectrum is multiplied by its own passband function P^k. These functions are calculated according to

$$\begin{cases} P^1_{i,j} = P^2_{i,j} = 1 & V \in [-s, +s] \\ P^1_{i,j} = 1 \quad \text{and} \quad P^2_{i,j} = 0 \quad \text{if} \quad V > +s \\ P^1_{i,j} = 0 \quad \text{and} \quad P^2_{i,j} = 1 & V < -s \end{cases},$$

$$V = \frac{E^1_{i,j}}{\sum_i^N \sum_j^N E^1_{i,j}} - \frac{E^2_{i,j}}{\sum_i^N \sum_j^N E^2_{i,j}}, \tag{1}$$

where (i,j) denotes the coordinates of a given pixel, N is the size of the image, $E^k_{i,j}$ is the spectral energy of an image k at the location (i,j), s is a given threshold, and $\sum_i^N \sum_j^N E^k_{i,j}$ is the spectral energy of the image k. For more target images, the different steps of the algorithm displayed in Fig. 1 should be repeated as many times as there are images.

To minimize the effect due to overlapping of the passband functions, a shifting operation of the different spectra is performed (Fig. 1) before each passband function is multiplied with its corresponding spectrum. The required shifting distance is calculated in order to remove overlapping in each signal's rms duration. The relevant shift distance, D_{shift}, is calculated versus the rms duration approximated by a 2D integral of the second moment of the signal [9] as

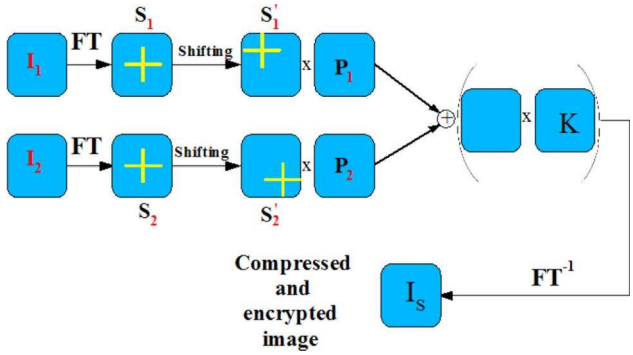

Fig. 1. (Color online) Synoptic diagram of the proposed simultaneously compressed and encrypted multiple-image algorithm.

$$\left(\frac{\Delta}{2}\right)^2 = \frac{1}{2\pi} \int_{-\infty}^{+\infty} \int_{-\infty}^{+\infty} |\nabla I(x,y)|^2 \mathrm{d}x\mathrm{d}y$$
$$= \int_{-\infty}^{+\infty} \int_{-\infty}^{+\infty} (u^2 + v^2) |S_I(u,v)|^2 \mathrm{d}u\mathrm{d}v, \tag{2}$$

where $S_I(u,v) = A(u,v)\exp(i\varphi(u,v))$ denotes the spectrum of the image $I(x,y)$ with the following property:

$$\frac{1}{2\pi} \int_{-\infty}^{+\infty} \int_{-\infty}^{+\infty} |S_I(u,v)|^2 \mathrm{d}u\mathrm{d}v = 1, \tag{3}$$

with $\nabla I(x,y)$ as the gradient, and $1/2\pi$ as a normalization factor. To achieve numerically our simulations, the right-hand side of Eq. (2) is discretized as $\sum_i^N \sum_j^N ((i - N/2)^2 + (j - N/2)^2)|S(i,j)|^2$.

In the next step, the shifted, segmented, and filtered spectra are merged together in the same Fourier plane (Fig. 1). Thus, we obtain one Fourier plane containing all spectra of the target images. Observe that, even after this first encryption stage, the system is still weak against attacks. By performing an inverse FT of the obtained plane, a (weakly) noisy superimposition of the target images is obtained. To increase the strength of the encryption algorithm, we first use one of the input multiple images as the first encryption key, e.g., picture of a fingerprint. The choice of this first key image is very important, because it must be more energetic than the target images and must contain enough information to properly hide the superimposition of the target images at the output plane. In our algorithm, the output is formed by a superimposition of the different target images and the first key image. Hence, if the key image is not encoded within the range [0–255], it is easy to make appear different parts of the target images. We further observe that the same situation can exist if the key image does not occupy all the space, i.e., if the key image is not present in some areas, only the superimposition of the different images exists. To increase further the encryption strength of the algorithm, a second encryption phase key (K in Fig. 1) was added to modify the spectral distribution of the segmented and filtered Fourier plane. This second key is calculated using biometric information of the authorized person to decrypt the images, i.e., a picture

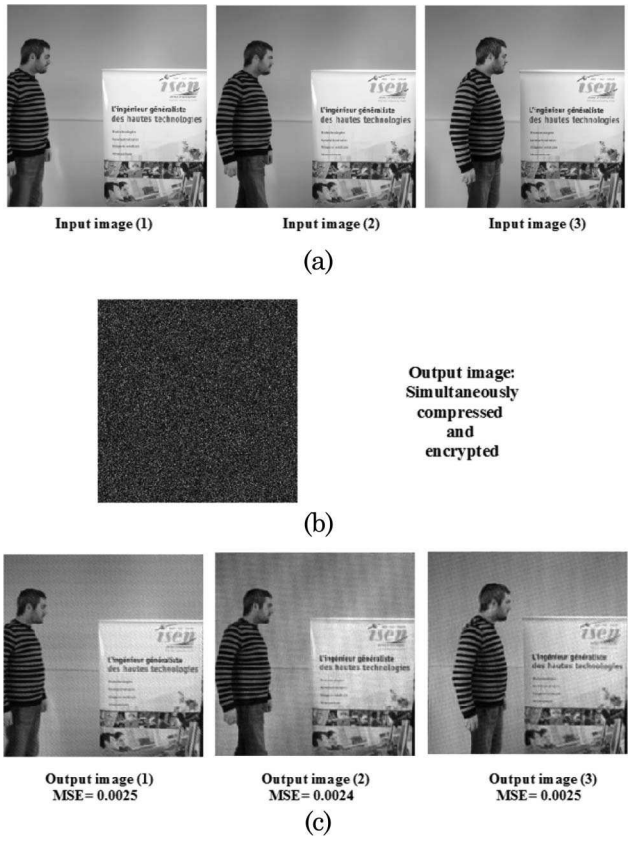

Fig. 2. (Color online) Images obtained using our algorithm: (a) target images, (b) encrypted and compressed image using two keys (a digital fingerprint at the input plane and a phase random key in the Fourier plane), and (c) decrypted and reconstructed images.

of his or her face. Consequently, both encryption keys will add strong noise to the output image (I_S in Fig. 1), ensuring a good encryption level.

To illustrate the good performance and simplicity of this algorithm, consider the three gray-level target images shown in Fig. 2(a). Each image has a size of 256×256 pixels and each pixel is coded on 8 bits. Thus, each image corresponds to $256 \times 256 \times 8$ bits. A fingerprint is used as the first encryption key. Using a random phase key as the second encryption key, we obtained the compressed and encrypted image shown in Fig. 2(b).

The amplitude and the phase of the output image were 8 bit coded, leading to a file to be transmitted and/or stored equal to $256 \times 256 \times 8 \times 2$ bits. The compression ratio, defined as the ratio of the size of the output file to the size of the three target images, is given by $T = \frac{256\times256\times8\times2}{256\times256\times8\times3} = \frac{2}{3}$. Note that the compression ratio of our algorithm is $T = \frac{2}{M}$, where M denotes the number of the target images. After transmitting the encrypted and compressed image [Fig. 2(b)], our algorithm involves the following three ingredients: (1) the inverse steps carried out in Fig. 1 should be performed, (2) the second encryption key should be known, and (3) the functions P_i should be known. The three decrypted images are shown in Fig. 2(c). These three images illustrate the good performance of our algorithm as evidenced by the good visual quality of the reconstructed images and by the values of the mean square error (MSE):

$$\mathrm{MSE} = \frac{1}{N \times N} \sum_{i}^{N} \sum_{j}^{N} |I_1'(i,j) - I_1(i,j)|^2 \approx 0.0025. \quad (4)$$

We point out that the close-to-zero MSE values are indications of the good performance of the criterion used in this study. Indeed, it allows a good distribution and allocation of information, i.e., in the Fourier plane, any image has the same weight as any other. We also tested this approach against several possible attacks using iterative algorithms to reconstruct images from their phases and/or their amplitudes [10]. The scheme is shown to be resistant against these brute force attacks, even after a large number of iterations. Furthermore, various tests performed using several types of images, e.g., color, have confirmed the good performance of our algorithm, but they are beyond the scope of this Letter.

This work was supported by Lab-STICC, which is Unité Mixte de Recherche CNRS 3192.

References

1. A. Alfalou and C. Brosseau, Adv. Opt. Photon. **1**, 589 (2009).
2. P. Réfrégier and B. Javidi, Opt. Lett. **20**, 767 (1995).
3. Y. Frauel, A. Castro, T. J. Naughton, and B. Javidi, Opt. Express **15**, 10253 (2007).
4. X. Yong-Liang, Z. Xin, Y. Sheng, L. Qiang, and L. Yang-Cong, Appl. Opt. **48**, 2686 (2009).
5. A. Alfalou and A. Mansour, Appl. Opt. **48**, 5933 (2009).
6. A. Alfalou, G. Keryer, and J. L. de Bougrenet de la Tocnaye, Appl. Opt. **38**, 6129 (1999).
7. B. V. K. V. Kumar, Digital Signal Process. **4**, 147 (1994).
8. B. V. K. V. Kumar and Z. Bahri, Appl. Opt. **28**, 250 (1989).
9. A. Papoulis, *The Fourier Integral and Its Applications* (McGraw-Hill, 1962).
10. A. V. Oppenheim and J. S. Lim, Proc. IEEE **69**, 529 (1981).